Exhibit Q

~~FOR OFFICIAL USE ONLY~~

(This slide UNCLASSIFIED)

Cellular Threats

Briefing for the Federal Mobile Technology Forum

Hosted by Federal CIO Council's Mobile Technology Tiger Team (MTTT)

6 February 2018

(b)(6); (b)(7)(C)

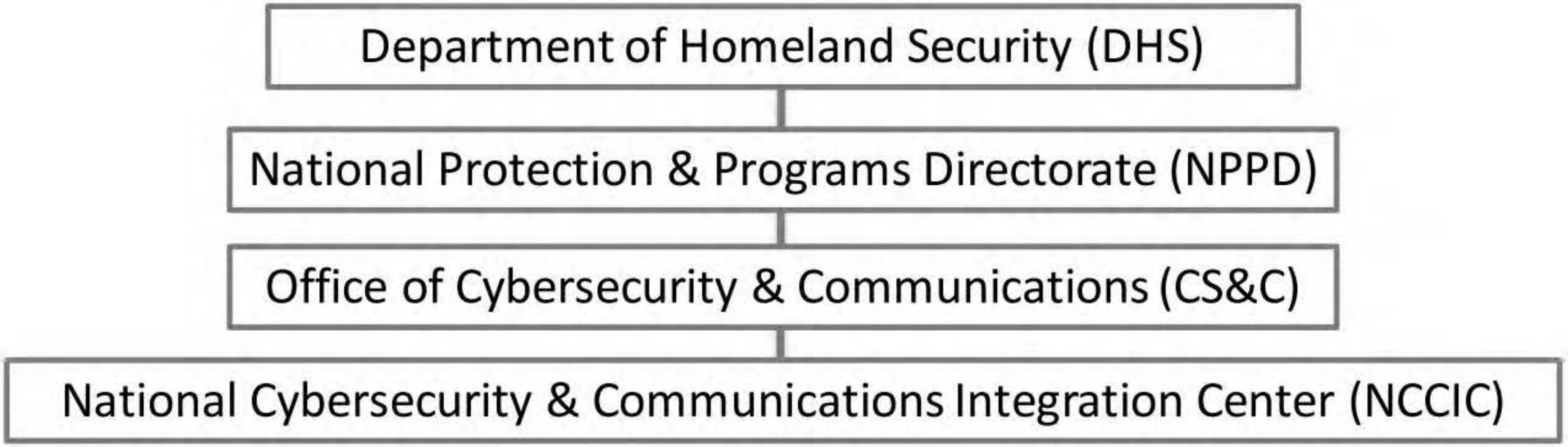
(b)(6); (b)(7)(C)

(b)(6); (b)(7)(C)

Homeland Security

National Coordinating Center for Communications (NCC)
National Cybersecurity & Communications
Integration Center (NCCIC)

National Cybersecurity & Communications Integration Center (NCCIC)



Department of Homeland Security (DHS)

National Protection & Programs Directorate (NPPD)

Office of Cybersecurity & Communications (CS&C)

National Cybersecurity & Communications Integration Center (NCCIC)

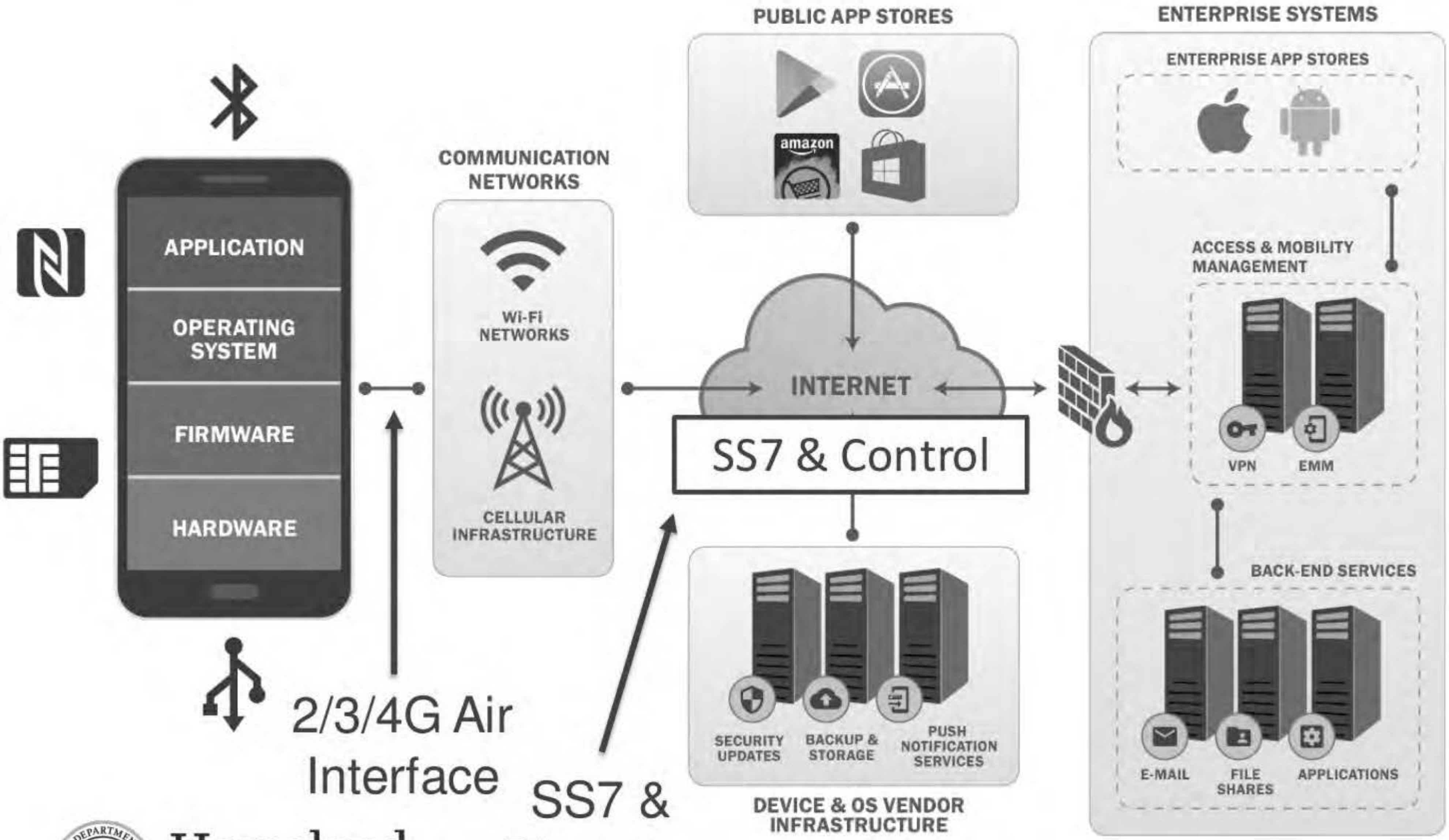
The NCCIC mission is to reduce the likelihood and severity of incidents that may significantly compromise the security and resilience of the nation's critical information technology and communications networks.

National Coordinating Center for Communications

- NCC is a joint government and industry partnership that coordinates efforts to protect, restore, and reconstitute communications infrastructures
- White House designated the NCC as the Information Sharing & Analysis Center (ISAC) for communications
- **The NCC facilitates the exchange of vulnerability, threat, and mitigation information amongst government and industry partners**

Homeland Security

Mobile Ecosystem & the focus of this brief



SS7 & Control

2/3/4G Air Interface

SS7 & Diameter

Homeland Security

What is SS7?

- Signaling System 7 is the set of protocols and systems used worldwide for:
  - Establishing/managing phone calls on landline and 2G/3G phones
  - Enabling Short Message Service (SMS) text messaging
  - Supports services like: 800 numbers, number portability, calling cards
- **5+ billion people use SS7; U.S. carriers use billions of SS7 messages/day**
  - **Issue 1: SS7 assumes trust between phone carriers worldwide**
  - **Issue 2: Many "bad actors" / "phone hackers" have access to SS7**
  - **Issue 3: Limited security controls are in place to prevent SS7 exploits**

~ 7.7 billion cell phone subscriptions (world pop = 7.6 B!)

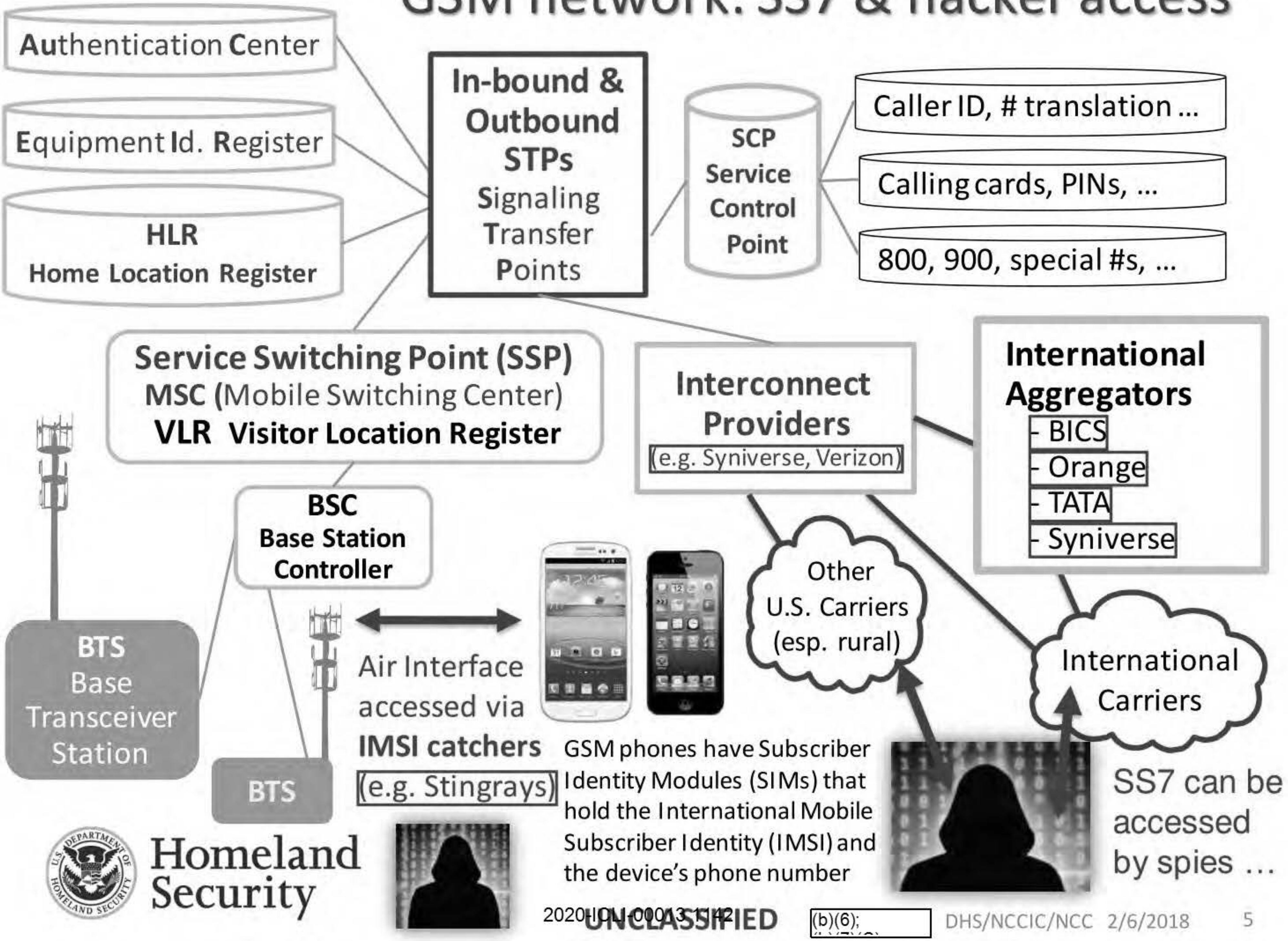
SS7 has more users than Internet*, but is less secure!

Significant, undetected exploits are possible

Homeland Security

* 2017 ITU estimate: 3.5 billion Internet users worldwide

GSM network: SS7 & hacker access



Authentication Center

Equipment Id. Register

HLR
Home Location Register

In-bound & Outbound STPs
Signaling Transfer Points

SCP
Service Control Point

Caller ID, # translation …

Calling cards, PINs, …

800, 900, special #s, …

Service Switching Point (SSP)
MSC (Mobile Switching Center)
VLR Visitor Location Register

Interconnect Providers
(e.g. Syniverse, Verizon)

International Aggregators
- BICS
- Orange
- TATA
- Syniverse

BSC
Base Station Controller

BTS
Base Transceiver Station

BTS

Air Interface accessed via **IMSI catchers** (e.g. Stingrays)

GSM phones have Subscriber Identity Modules (SIMs) that hold the International Mobile Subscriber Identity (IMSI) and the device's phone number

Other U.S. Carriers (esp. rural)

International Carriers

SS7 can be accessed by spies …

Homeland Security

2008 - 2016: Examples of SS7 risks in media

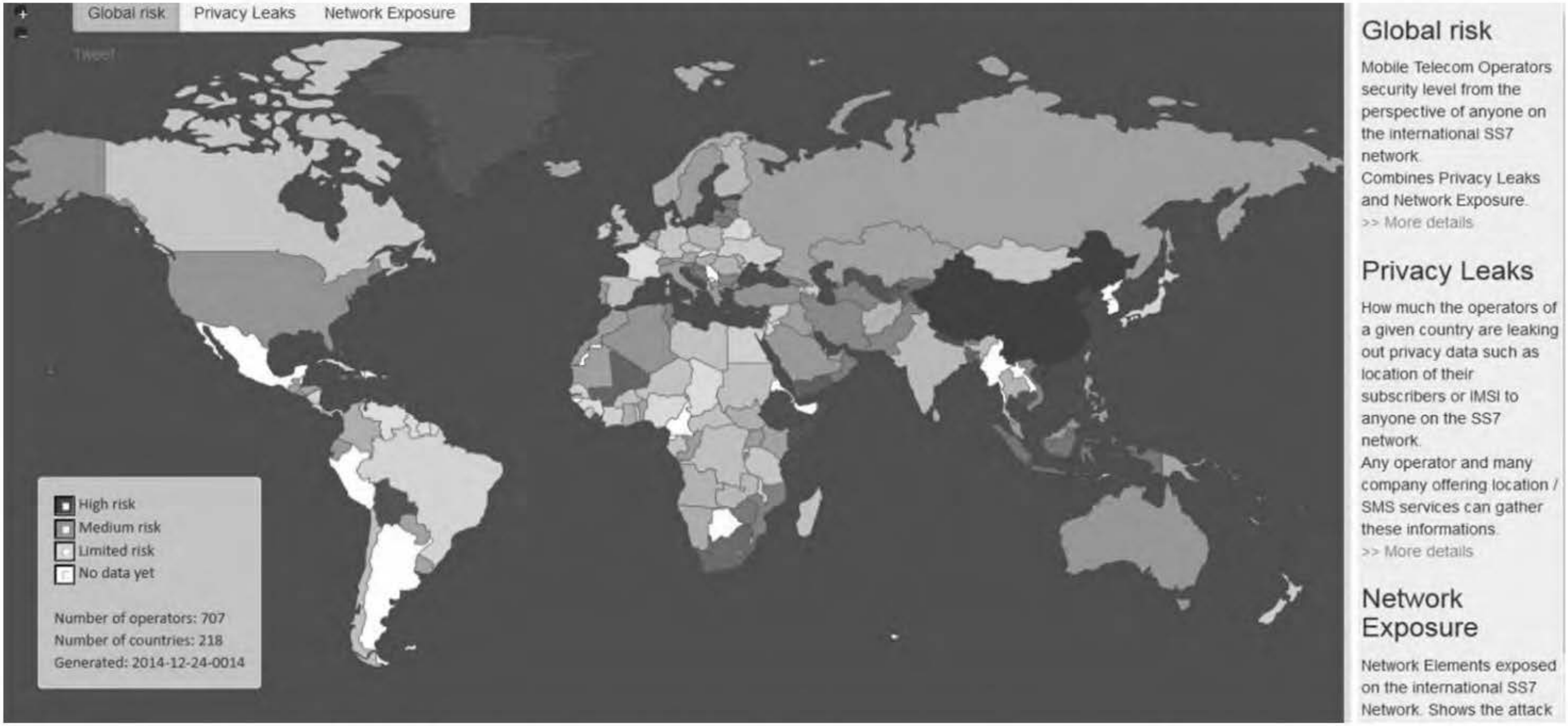
- **2008**: Chaos Communications Congress (CCC) – Tobias Engel: "Locating Mobile Phones using Signalling System #7" https://events.ccc.de/congress/2008/Fahrplan/attachments/1262_25c3-locating-mobile-phones.pdf
- 2011: CCC - Karsten Nohl – Exploiting calls + SMS* https://www.youtube.com/watch?v=ZrbatnnRxFc
- 2013: K. Nohl on SIM* risks http://michaelkreil.github.io/30c3-slides/slides_jpeg/saal1/2013-12-27T17-25-51.jpg
- **2014**: Year of more detailed risk explanations to public – greater focus at CCC
  - August - Washington Post: "*For sale: Systems that can secretly track where cellphone users go around the globe*" www.washingtonpost.com/business/technology/for-sale-systems-that-can-secretly-track-where-cellphone-users-go-around-the-globe/2014/08/24/f0700e8a-f003-11e3-bf76-447a5df6411f_story.html
  - December - CCC (31c3) had three talks on cell phone SS7 related vulnerabilities
  - ZDNet "*Invasive phone tracking: New SS7 research blows the lid off mobile security*" www.zdnet.com/article/invasive-phone-tracking-new-ss7-research-blows-the-lid-off-personal-security/
- 2015: 60 Minutes Australia's episode on SS7 and IMSI*-catcher risks www.news.com.au/technology/gadgets/the-end-of-privacy-as-we-know-it-60-minutes-uncovers-huge-mobile-phone-security-vulnerabilities/story-fn6vihic-1227485884359
- **2016: 60 Minutes "Hacking Your Phone" episode aired in USA** (aired 4/17/16)
  - Daily Beast reporting/reaction on SS7 phone issues and A/S Ozment's hearing www.thedailybeast.com/articles/2016/04/23/here-s-why-anyone-could-hack-your-phone.html

Homeland Security

* SMS = Short Message Service IMSI = International Mobile Subscriber Identity
SIM = subscriber identity module or subscriber identification module [see slide notes for more details]

2014: SS7 risk awareness – SS7Map Global Risk

SS7Map assessed how well cellphone companies were safeguarding subscriber data. **The US was classified as a "medium risk".**



Number of operators: 707
Number of countries: 218
Generated: 2014-12-24-0014

Global risk

Mobile Telecom Operators security level from the perspective of anyone on the international SS7 network.
Combines Privacy Leaks and Network Exposure.
>> More details

Privacy Leaks

How much the operators of a given country are leaking out privacy data such as location of their subscribers or IMSI to anyone on the SS7 network.
Any operator and many company offering location / SMS services can gather these informations.
>> More details

Network Exposure

Network Elements exposed on the international SS7 Network. Shows the attack

[Note: P1 Security (a French firm) produced this map; see http://ss7map.p1sec.com]

2015 threat example: OPM data breach

- Office of Personnel Management (OPM) data breaches impacted those who applied for clearances along with their associates (over 21 million people's personal data compromised)
- **Compromised data included:**
  - Age and Address
  - Relationships
  - Home/work phone numbers
  - **Cell phone numbers**

- In 2015, **Chinese government arrested some hackers** it says were connected to the breach of OPM's database
- In 2017, the **FBI arrested a Chinese national** connected to the Sakura malware used in the OPM data breach

Homeland Security

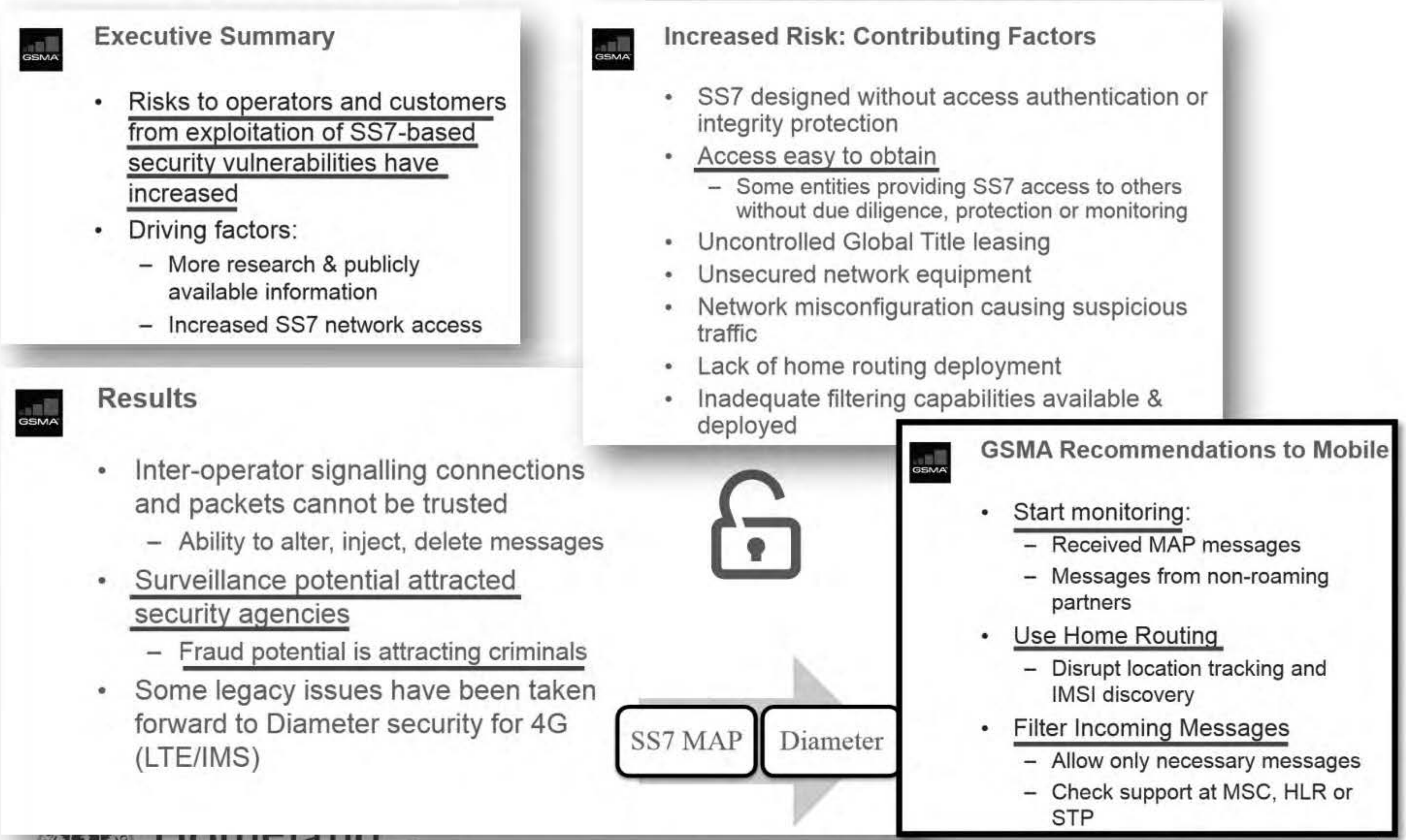
Reported 2015 SS7 anomalous traffic Possibly related to OPM breach

(b)(7)(E)

Note: This is preliminary data and does not represent all suspicious SS7 traffic that occurred during the summer of 2015

Homeland Security

2016 GSMA brief on SS7 Interconnect Security



Executive Summary

- Risks to operators and customers from exploitation of SS7-based security vulnerabilities have increased
- Driving factors:
  - More research & publicly available information
  - Increased SS7 network access

Increased Risk: Contributing Factors

- SS7 designed without access authentication or integrity protection
- Access easy to obtain
  - Some entities providing SS7 access to others without due diligence, protection or monitoring
- Uncontrolled Global Title leasing
- Unsecured network equipment
- Network misconfiguration causing suspicious traffic
- Lack of home routing deployment
- Inadequate filtering capabilities available & deployed

Results

- Inter-operator signalling connections and packets cannot be trusted
  - Ability to alter, inject, delete messages
- Surveillance potential attracted security agencies
  - Fraud potential is attracting criminals
- Some legacy issues have been taken forward to Diameter security for 4G (LTE/IMS)

GSMA Recommendations to Mobile

- Start monitoring:
  - Received MAP messages
  - Messages from non-roaming partners
- Use Home Routing
  - Disrupt location tracking and IMSI discovery
- Filter Incoming Messages
  - Allow only necessary messages
  - Check support at MSC, HLR or STP

Homeland Security

(b)(6); (b)(7)(C)

2016: Telenor incident / US networks have similar risks!

(b)(7)(E)

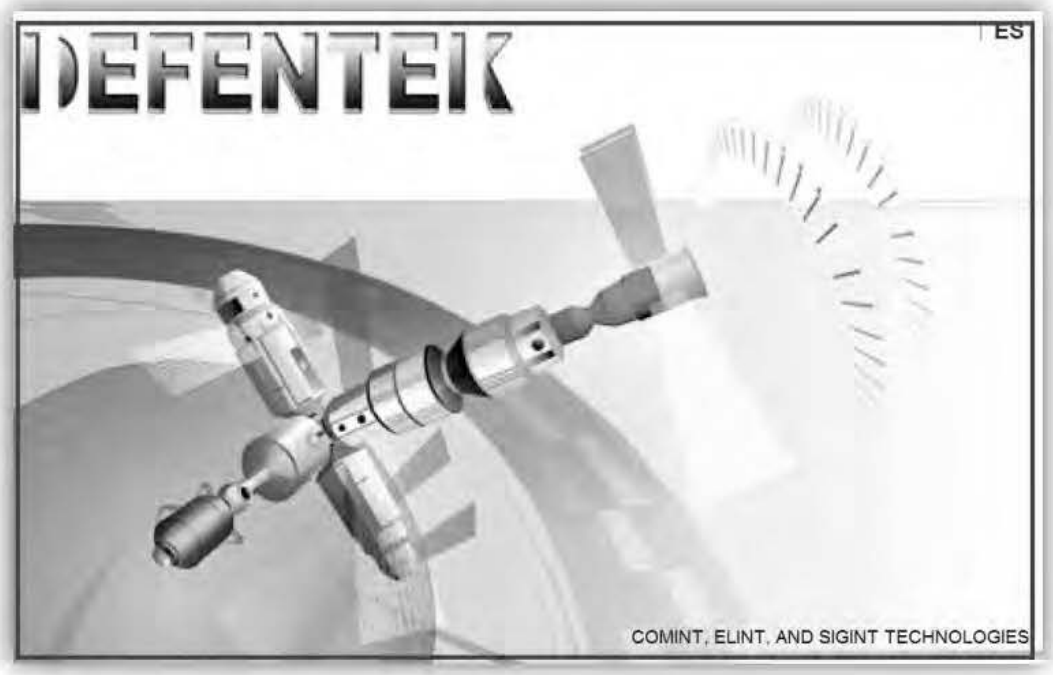
Homeland Security

Note: used by permission of source

(b)(7)(E)

(b)(7)(E)

2016: Cell phone exploits advertised on the Internet: note … this site is no longer available



From www.defentek.com:

"The ***Infiltrator*** is a … solution for collecting, analyzing and presenting the status of any mobile user status & location. The ***Infiltrator*** gives a clear location and movement of anyone anywhere in the world. Even if the SIM card is switched out, we are actually tracking the handset thereafter. Additional modules allows to remotely activate the speaker on the handset and capture all of the surrounding conversation anywhere in the world where the hand set is located, and no matter how many times the SIM card is switched or replaced."

Homeland Security

(b)(7)(E)

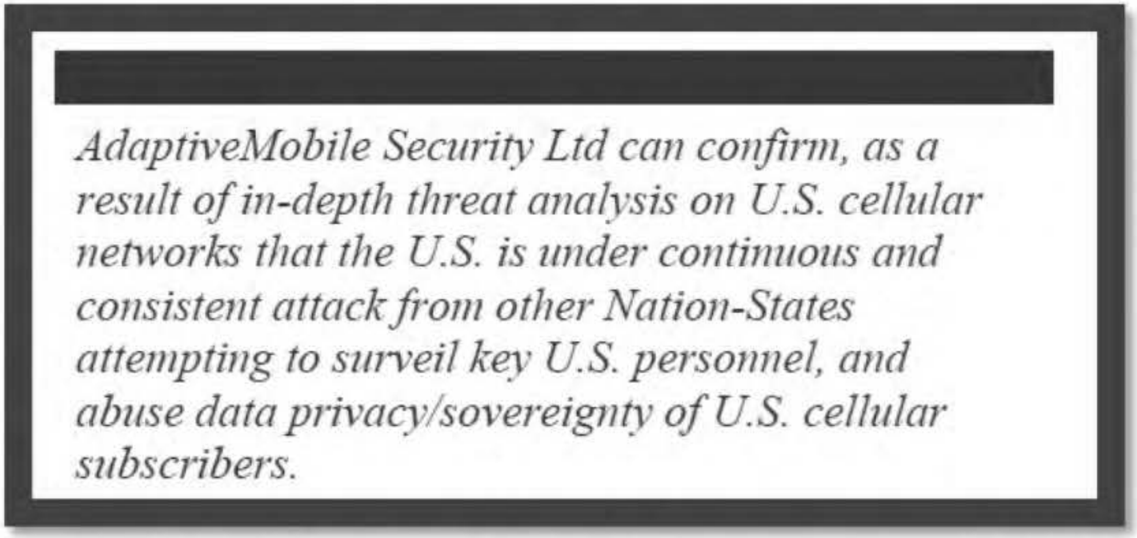
Homeland Security

Note: used by permission of source

(b)(7)(E)

Note: Derived/used by permission of source

April-May 2017: DHS Mobile Device Security Report



[redacted]

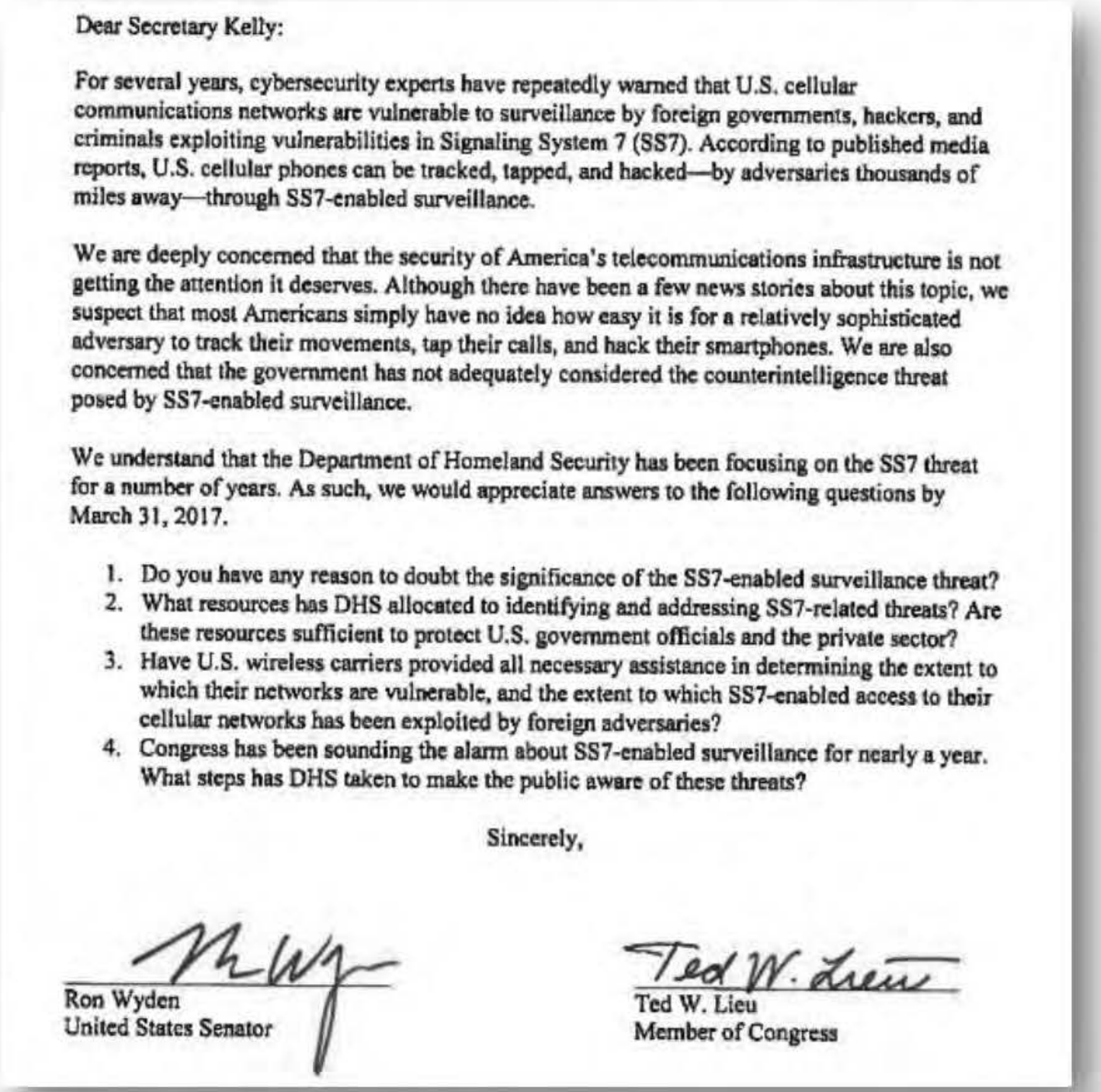
AdaptiveMobile Security Ltd can confirm, as a result of in-depth threat analysis on U.S. cellular networks that the U.S. is under continuous and consistent attack from other Nation-States attempting to surveil key U.S. personnel, and abuse data privacy/sovereignty of U.S. cellular subscribers.

- *"Threats to the Government's use of mobile devices are real and exist across all elements of the mobile ecosystem."*
- *"Gaining unauthorized access to the core SS7 or Diameter network is a risk since there are tens of thousands of entry points worldwide, many of which are controlled by countries or organizations that support terrorism or espionage."*
- *"A number of threats against SS7 have been publicly described, including the ability to determine the physical location of cellular mobile devices, disrupt phone service from individual phones to entire networks, intercept or block SMS text messages, and redirect or eavesdrop on voice conversations."*

March 2017: Congressional letter to DHS S1

"… According to published media reports, U.S. cellular phones can be tracked, tapped, and hacked …

We are deeply concerned that the security of America's telecommunications infrastructure is not getting the attention it deserves. …"



Dear Secretary Kelly:

For several years, cybersecurity experts have repeatedly warned that U.S. cellular communications networks are vulnerable to surveillance by foreign governments, hackers, and criminals exploiting vulnerabilities in Signaling System 7 (SS7). According to published media reports, U.S. cellular phones can be tracked, tapped, and hacked—by adversaries thousands of miles away—through SS7-enabled surveillance.

We are deeply concerned that the security of America's telecommunications infrastructure is not getting the attention it deserves. Although there have been a few news stories about this topic, we suspect that most Americans simply have no idea how easy it is for a relatively sophisticated adversary to track their movements, tap their calls, and hack their smartphones. We are also concerned that the government has not adequately considered the counterintelligence threat posed by SS7-enabled surveillance.

We understand that the Department of Homeland Security has been focusing on the SS7 threat for a number of years. As such, we would appreciate answers to the following questions by March 31, 2017.

1. Do you have any reason to doubt the significance of the SS7-enabled surveillance threat?
2. What resources has DHS allocated to identifying and addressing SS7-related threats? Are these resources sufficient to protect U.S. government officials and the private sector?
3. Have U.S. wireless carriers provided all necessary assistance in determining the extent to which their networks are vulnerable, and the extent to which SS7-enabled access to their cellular networks has been exploited by foreign adversaries?
4. Congress has been sounding the alarm about SS7-enabled surveillance for nearly a year. What steps has DHS taken to make the public aware of these threats?

Sincerely,

Ted W. Lieu

Ron Wyden
United States Senator

Ted W. Lieu
Member of Congress

Homeland Security

June 2017 - VoLTE is vulnerable

BleepingComputer June 12, 2017 article:

"A team of researchers from French company P1 Security has detailed a long list of issues with the 4G VoLTE telephony, a protocol that has become quite popular all over the world in recent years and is currently in use in the US …

VoLTE stands for Voice Over LTE – where LTE stands for Long-Term Evolution and is a high-speed wireless communication for mobile phones and data terminals, based on older GSM technology.

Researchers say they identified both "active" vulnerabilities (that require modifying special SIP packets) and "passive" vulnerabilities (that expose data via passive network monitoring or do not require any SIP packet modification)."

Note: FirstNet uses VoLTE technology

Sources: (1) https://www.bleepingcomputer.com/news/security/hackers-can-spoof-phone-numbers-track-users-via-4g-volte-mobile-technology/
(2) P1 Security published "Subscribers remote geolocation and tracking using 4G VoLTE enabled Android phone" in June 2017. https://www.sstic.org/media/SSTIC2017/SSTIC-actes/remote_geolocation_and_tracing_of_subscribers_usin/SSTIC2017-Article-remote_geolocation_and_tracing_of_subscribers_using_4g_volte_android_phone-le-moal_ventuzelo_coudray.pdf

Homeland Security

(b)(7)(E)

(b)(7)(E)

Note: used by permission of source

Cellular Threats

(b)(7)(E)

Note: used by permission of source

NCC Cellular Pilot Update: "Overwatch" in NCR

(b)(7)(E)

Sensors detect IMSI catchers

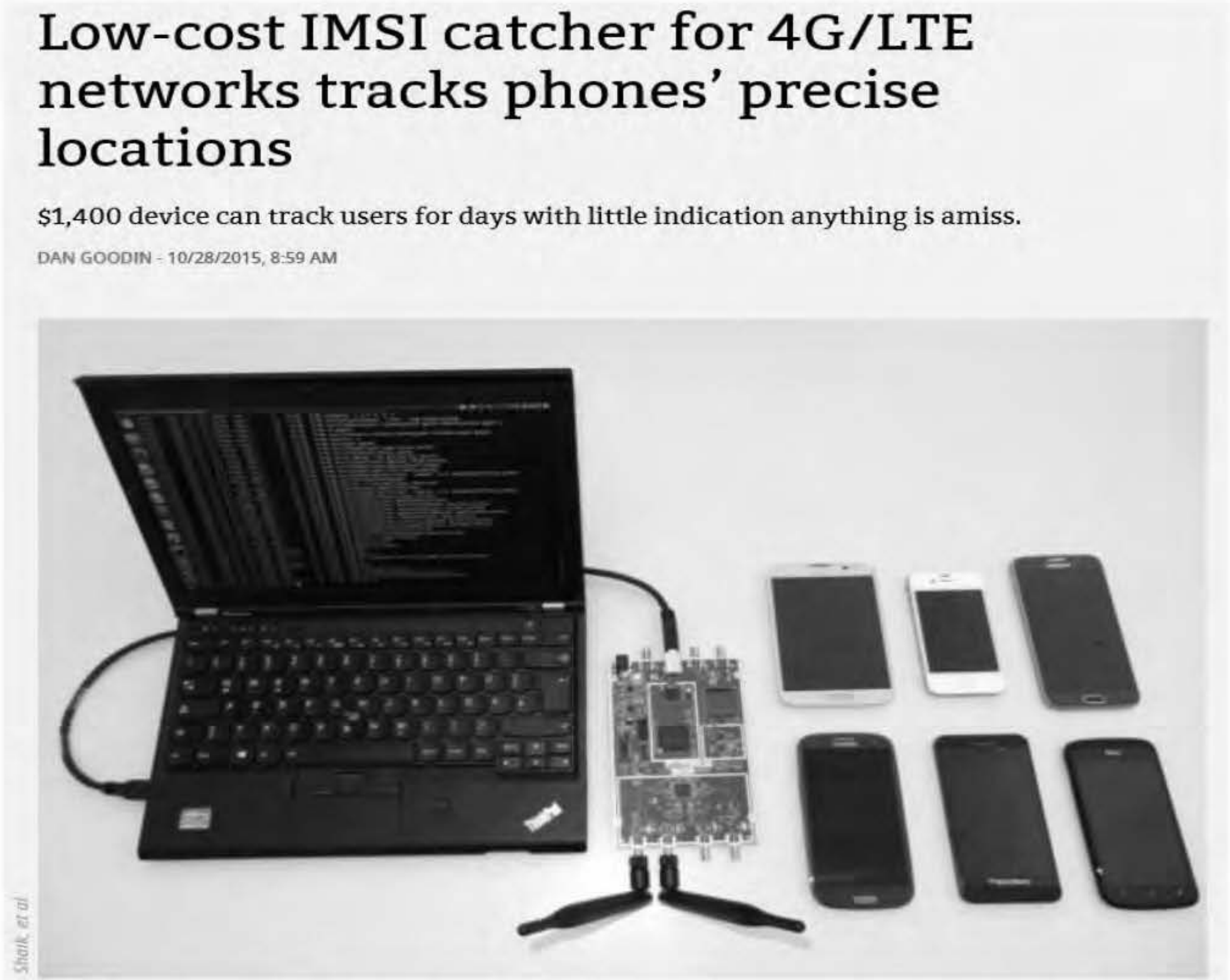
- NCC Pilot detects, characterizes, and geo-locates legitimate and rogue cellular base stations (also known as IMSI catchers) in the National Capital Region
- Reportedly: "*first and only strategic real-time IMSI catcher detection system*"

(b)(7)(E)

Homeland Security

(b)(6); (b)(7)(C)

Threat 1: Low-cost rogue cellular base stations



Low-cost IMSI catcher for 4G/LTE networks tracks phones' precise locations

$1,400 device can track users for days with little indication anything is amiss.

DAN GOODIN - 10/28/2015, 8:59 AM

Shaik et al

"The equipment can cause all LTE-compliant phones to leak their location to within a 32- to 64-foot radius ... operating a rogue base station... total cost" ... about $1,400

https://arstechnica.com/security/2015/10/low-cost-imsi-catcher-for-4glte-networks-track-phones-precise-locations/

Homeland Security

* IMSI = International Mobile Subscriber Identity

Threat 2: Sophisticated rogue cellular base stations

- Example: (b)(7)(E) (b)(7)(E) can intercept, record, & track cell phones/devices
- Range: hundreds of meters
- (b)(7)(E) also (b)(7)(E) "IMSI* catchers"
  - Detect mobile phones & extract their identities (e.g. IMSIs)
  - Can be wearable or used in cars or airborne platforms
  - Can be used with direction finders
  - Can also exploit phones on CDMA* networks and GSM* networks

Sources: (b)(7)(E) and other pages on that site

* **CDMA** = Code Division Multiple Access; **GSM** = Global System for Mobile Communications; **IMSI** = International Mobile Subscriber Identity;

Homeland Security

NCC Rogue Cellular Pilot findings: (b)(7)(E)

August 23, 2016: Detected likely IMSI catcher monitoring/tracking phones (b)(7)(E)

- Potential IMSI catcher emulating an existing tower on (b)(7)(E)

(b)(7)(E)

Pilot findings – (b)(7)(E) rogue cell in VA

(b)(7)(E)

Possible rogue cell (b)(7)(E) – 30 Aug 2017

(b)(7)(E)

Cellular Threats

(b)(7)(E)

Conclusions / General Way Ahead

- Government & industry must continue to work together to address threats
  - Tracking and monitoring of leaders, staff, and public; (b)(7)(E)

(b)(7)(E)

- Don’t take cell phones into sensitive meetings (or use Faraday bags/boxes)
- Users can mitigate their risks through exploit resilient end devices and Apps
- Can use phone service contracts that require SS7 monitoring/filtering/reporting
- Need sophisticated monitoring/filtering (b)(7)(E)

Homeland Security

Need **comprehensive** monitoring/blocking of malicious traffic and trust based on **verification**